Date of Hearing: April 17, 2007

ASSEMBLY COMMITTEE ON JUDICIARY
Dave Jones, Chair
AB 779 (Jones) – As Amended: April 10, 2007

SUBJECT: PERSONAL INFORMATION: STATE AGENCIES AND BUSINESSES

KEY ISSUES:

1) SHOULD RETAILERS BE PROHIBITED FROM RETAINING A CONSUMER'S PERSONAL INFORMATION FOR LONGER THAN 90 DAYS AFTER A TRANSACTION?

2) WHEN A PERSON OR ENTITY IS REQUIRED TO NOTIFY AN INDIVIDUAL THAT HIS OR HER PERSONAL INFORMATION HAS BEEN COMPROMISED, SHOULD THE NOTICE BE WRITTEN IN PLAIN ENGLISH AND INCLUDE BASIC INFORMATION ABOUT THE NATURE OF THE BREACH?

3) SHOULD A PERSON OR BUSINESS THAT OWNS OR LICENSES PERSONAL INFORMATION BE PERMITTED TO RECOVER THE REASONABLE COSTS OF NOTIFICATION FROM THE PERSON OR BUSINESS THAT MAINTAINED AND COMPROMISED THE PERSONAL INFORMATION?

SNYOPSIS

This bill seeks to make three changes to California's breach notification law. While the author believes that the law has shown its value in the three years that it has been in effect, experience has also revealed a few aspects of the law that could be improved. First, this bill would entitle a person or business that owns or licenses personal information to seek reimbursement for notification costs from the person or business that actually maintained and compromised the information. Under the existing notification law the owner or licensee is required to provide notice, even if someone else maintained the information and was responsible for the breach. This bill would not change this, but it would permit the owner or licensee to seek reimbursement. Second, this bill seeks to improve the notification law by making the notice itself more user-friendly, requiring that it be written in plain English and provide necessary information to a person whose information has been compromised. Finally, this bill prohibits a retail seller from retaining the personal information of consumers for more than 90 days after a transaction. By limiting the amount of time that retailers hold consumer information, the bill seeks to reduce the likelihood that a data breach will occur in the first place. The bill is sponsored by California Credit Union League, since credit unions are required to notify customers of a data breach even though a retailer may have comprised the information. Opponents of this bill include a number of retail and financial associations.

SUMMARY: Makes changes designed to improve California's data security breach notification law. Specifically, this bill:

1) Clarifies that a retail seller that collects and maintains personal information for any purpose is subject to the breach notification law and prohibits a retail seller from retaining personal information for longer than 90 days after the date of the transaction.

2) Requires that a copy of the breach notification be provided to the Office of Privacy Protection. Provides further that the breach notification must be written in plain English and shall include, at a minimum, all of the following:

   a) The date of the notice;
   b) The name of the agency that maintained the data at the time of the breach;
   c) The date on which the breach occurred;
   d) A description of the categories of personal information that may have been compromised;
   e) A toll-free number or an electronic mail address that the individual may use to contact the person, entity, or agency responsible for the breach;
   f) The toll-free numbers and addresses of the major credit reporting agencies.

3) Provides, if breach notification is required, that the owner or licensee of the personal information shall be entitled to reimbursement from the person or business that maintained the data for all reasonable and actual costs of providing notice to consumers.

EXISTING LAW:

1) Requires any person, business, or government agency that owns or licenses computerized personal information to disclose any breach in the security of that data to any California resident whose unencrypted personal information was disclosed to, or acquired by, an unauthorized person. Provides further that notice of breach shall be made in the most expedient time possible, unless a law enforcement agency determines that notification will impede or compromise a criminal investigation. (Civil Code Sections 1798.29 (a) and (c) and 1798.82 (a) and (c).)

2) Requires any person, business, or government agency that maintains, but does not own or license, computerized personal information, to notify the owner or licensee in the event of a security breach. (Civil Code Sections 1798.29 (b) and 1798.82 (b).)

3) Requires persons and businesses that conduct business in California, and who own or license the personal information of their customers, to implement and maintain reasonable security measures to protect that information and, subject to certain conditions, to notify customers as to any disclosures of that information to third parties. Provides further that if a person or business discloses personal information pursuant to a contract with a third party, the person or business shall require by contract that the third party implement and maintain reasonable security practices and procedures. (Civil Code Section 1798.81.5.)

4) Defines "personal information," for purposes of the breach notification law, to include the person's first and last name, or first initial and last name, in combination with any of the following: a social security number, driver's license number, and certain account numbers if disclosed in combination with corresponding access codes. Specifies that personal information does *not* include publicly available information that is publicly available in federal, state, or local government records. (Civil Code Sections 1798.29 (e)-(f) and 1798.82 (e)-(f).)

5) Provides that any person, business, or government agency that notifies subject persons in accordance with its own information security policy shall be deemed in compliance with the breach notification law, so long as the policy is otherwise consistent with the timing requirements of the law. (Civil Code Sections 1798.29 (h) and 1798.82 (h).)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: According to the author and sponsor, this bill makes needed improvements to California's landmark data breach notification law in light of three years of experience with the operation of the law. The bill makes three important changes to existing law: (1) it entitles the owner or licensee of personal information to recover notification costs from the person or business that actually maintained and compromised the data; (2) it clarifies that retail sellers are subject to the notification law and limits that time that they can retain personal information; (3) it requires notices to be more consumer-friendly.

Reimbursement Provision: Existing law generally requires a person or business that owns or licenses computerized data that contains an individual's personal information to notify that individual in the event of a security breach. (Civil Code Section 1798.82 (a).) While the person or business that *owns or licenses* that data is often the same person or business that *maintains* the data, this is not always the case. For example, when a bank or credit union issues an ATM card or credit card it "owns" the personal information contained on that card for purposes of the law. However, if the consumer swipes that card at a retail store that information is maintained by the retailer for some period of time. If the personal information is breached while in possession of the retailer, it is still the owner or licensee who must notify the consumer of the breach. The retailer, or any other person or business that maintains the personal information, is only required to notify the owner or licensee; the burden then falls to the owner or licensee to notify the affected consumers. (Civil Code Section 1798.82 (b).)

Since these breaches can sometimes involve thousands of people, notification can be quite costly. By giving the owner or entity the right to recover notification costs from the party that actually compromised the data, the author contends that this bill "introduces responsibility and compensation . . . inasmuch as entities that are not sufficiently protective of consumer data will have to pay for the reasonable and actual costs to those who have to provide notice to consumers." Giving the owners and licensee this right to reimbursement is not only a matter of fairness; the author believes that this measure will also "act as a financial incentive for entities to take better care of consumer personal information."

Provision Relating to Retail Sellers: This bill clarifies that a retail seller that collects or maintains personal information – such as when it acquires the information from a swiped card and then retains that information – is subject to the breach notification and data protection laws. It appears that retail sellers are already covered by the current law (Title 1.81 of Part 4 of Civil Code commencing with Section 1798.80), which defines covered businesses to include "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate for a profit." However, this bill will simply make it clear that when a retailer collects and retains personal information from its customers, it maintains personal information for purposes of the law.

More significantly, this bill prohibits retail sellers from retaining personal information for longer than 90 days from the date of the transaction. According to the author, this provision of the bill "seeks to limit the amount of time that entities hold onto consumer information, since we know that the longer unnecessary information is stored, the more likely a data breach is to occur."

Provisions Relating To the Contents of the Notification: Existing law prescribes the *methods* by which notice shall be given but says nothing about the required *contents* of the notice. Under existing law, a person or entity must provide notice "in the most expedient time possible and without unreasonable delay," unless a law enforcement agency determines that notification will impede a criminal investigation. (Civil Code Sections 1798.29 (a) and1798.82 (a).) It permits both written and electronic notice, so long as the latter is consistent with requirements for "electronic signatures" as set forth in Section 7001 of Title 15 of the United States Code. It also permits "substitute notice" if a person or entity demonstrates that the cost of notice would exceed $250,000 or if the number of persons affected exceeds 500,000, or if the person or business does not have sufficient contact information to notify the affected persons individually. Substitute notice can include posting the notice on a website or publication in major statewide media. (Civil Code Sections 1798.29(g) and 1798.82(g).) But as to the content of the notice, the only apparent requirement in existing law is acknowledgement that a security breach has in fact occurred.

This bill seeks to add some "modest and reasonable" requirements that will make the notice itself more helpful and useful to the consumer whose information has been breached. The author claims that some data breach notices "do not even have the date of the letter, let alone the date of the breach." This bill will require the notice to include the date of the breach, the name of the person, business or agency that maintained the data at the time of the breach, and the kinds of personal information that may have been compromised. In addition, the notice has to include helpful information to the consumer, including a toll-free number and address for contacting the person, business, or agency that maintained the data and toll-free numbers and addresses of the major credit reporting agencies. This information will permit the affected individual to more quickly take appropriate steps to mitigate possible damages.

ARGUMENTS IN SUPPORT: According to the author the three provisions of this bill will achieve three important objectives. First, by giving owners and licensees the right to seek reimbursement from the party that compromised the data, it creates a financial incentive for businesses to take better care of its customers' personal information. Second, it will make the notices themselves more consumer-friendly. Third, it will decrease the amount of time that retailers retain personal information and thereby reduce the probability that the information will be subject to a data breach.

The author also argues that during the three years in which the notice law has been in effect, we have learned a great deal about its strengths and shortcomings. In particular the author points to two areas where experience suggests a need for modest reforms. The author writes,

> First, it has become clear that a number of entities are simply not adequately protecting consumer personal information in such a way to minimize or mitigate security breaches. For example, TJX Companies, Inc., parent company to TJ Maxx, Marshalls and other retail establishments, announced on March 29 of this year that a security breach previously thought to be relatively limited in scope in fact involved the theft of 45.6 million credit and debit card numbers stolen over an 18-month period,

> making it the biggest security breach ever . . . AB 779 creates a financial incentive for entities to better protect consumer data by 1) making responsible entities pay for the "reasonable and actual costs" of providing security breach notices to consumers and 2) limiting the amount of time that retailers can retain personal information to 90 days after a transaction.
>
> Second, there are some modest and reasonable steps that can be taken to enhance the actual breach notices themselves that consumers may receive . . . To that end AB 779 includes a number of suggestions to enhance the quality of information that consumers receive pursuant to a data breach. These include providing a copy of the breach notice to California's Office of Privacy Protection within the Department of Consumer Affairs, and ensuring that a breach notice includes useful consumer information such as toll-free numbers that consumers may consult to protect themselves from ID theft stemming from data breaches. The items in this part of the bill are consistent with those contained in bipartisan legislation currently pending in the U.S. Congress. Consumers, once armed with more detailed information about who is responsible for data breaches that impact their personal information and subject them to additional ID theft risk, may well decide to avoid patronizing businesses that fail to adequately protect their personal information.

The California Credit Union League, who sponsors this bill, argues that this measure will "enhance California's existing data breach notification law." In particular, the sponsor believes that this bill addresses three deficiencies that are especially important to credit unions. First, the sponsor believes that this bill will force retailers to take greater steps to secure financial data and limit the opportunities for data breaches to occur. Second, the revamped notice requirement will mean that consumers will have the correct information about where data breeches occur. This is particularly important to credit unions, because even though the retailer might be responsible for the breach, existing law requires the credit union to provide the notice to the consumer. The consumer, the credit unions fear, will equate the message with the messenger, creating bad public relations for the credit union even though it was not responsible for the breach. Finally, the sponsor supports the reimbursement provision, not only because it is fairer but also because, again, it creates pressure for merchants to prevent data breaches.

ARGUMENTS IN OPPOSITION: Opponents of this bill include a number of retail and financial associations. They argue that "this bill would prohibit virtually any entity in California from maintaining a customer database or mailing list of any sort." Opponents claim that this measure could even prevent a business from maintaining names and information for the purpose of providing customers with a monthly billing service, even where the customer has provided the personal information to the business for that purpose.

Opponents also complain that this bill requires different reporting requirements for businesses and state agencies. In fact, this does not appear accurate. Reporting and notice requirements appear to be the same for both businesses and state agencies, except for the requirement that retailers purge personal information after 90 days. It does appear to be the case, however, that businesses and state agencies are treated differently under the reimbursement provisions of this bill. Those provisions appear to apply only to businesses, not to state agencies. This distinction may be justified, however, if state agencies are more likely to be both the entity that "owns and licenses" the data and the entity that "maintains" the data, since the reimbursement provision is only relevant if the entity that owns or licenses the data is distinct from the one that maintains it.

Such a separation is not uncommon among private businesses, as in the case of the credit union which owns the data and the retailers that collect the data from its cards. The Committee, however, has been unable to determine whether or not state agencies very often maintain data that is owned or licensed by someone else.

Finally, opponents oppose the reimbursement provision of this bill. They claim that this provision amounts to unwarranted government interference between consenting businesses that have contractual agreements and obligations.

However, it should be pointed out that this argument presumes that there is in fact always a contractual agreement between the owner of the data and the maintainer of the data. According to the sponsor, credit unions issue debit and credit cards that can be swiped by retailers anywhere. While credit card companies like Visa or MasterCard have a contractual relationship with retailers that accept their cards, the credit union that issues the card does not have a contract with the retailer. Also, in the case of a debit card, which is also swiped by retailers, there is certainly no contract between the credit union and every retailer who might accept it. Yet if the data is breached while in the possession of the retailer, it is the credit union that must bear the costs of notification, even if it was not at all responsible for the breach.

PENDING AND RECENT RELATED LEGISLATION: AB 512 (Lieber), 07-08 session, adds private medical or health care records to the list of personal information subject to California's breach notification law. The bill was double-referred to the Judiciary and B&P Committees.

AB 1298 (Jones), 07-08 session, adds, among other provisions, medical information and health insurance information to the list of personal information subject to California's breach notification law. This bill passed the Assembly Judiciary Committee on April 10, 2007.

SB 364 (Simitian), 07-08 session, lowers the dollar threshold for the "substitute notice" provision of the data breach law from $250,000 to $100,000. This bill has been referred to the Senate Judiciary Committee but has yet to be set for hearing.

AB 786 (Ruskin), 05-06 session, would have provided CSU employees with four hours of time off with pay to minimize damages stemming from a data breach. The bill died in Assembly Appropriations.

AB 2505 (Nuñez), 05-06 session, would have additionally required notification of the Office of Privacy Protection in the Department of Consumer Affairs when an entity uses the "substitute notice" provision of the data breach law (e.g. when notice costs would be more than $250,000 or more than 500,000 people would have to be notified or when the entity does not have sufficient contact information on those consumers affected). This bill died on the Senate floor.

SB 852 (Bowen), 05-06 session, would have triggered the data breach notification provision irrespective of whether the data was computerized or not. It also would have required the Office of Privacy Protection to receive a copy of the notice sent to the consumer. This bill failed at the Assembly Business and Professions Committee.

SB 1512 (Machado), 05-06 session, would have increased the dollar threshold for the "substitute notice" provision from $250,000 to $500,000. This bill was never heard after being referred to the Senate Judiciary Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

California Credit Union League (sponsor)
American Civil Liberties Union
American Federation of State, County and Municipal Employees
Consumer Federation of California
Consumers Union

Opposition

California Bankers Association
California Retailers Association
California Financial Services Association
California Grocers Association
California Mortgage Bankers Association
California Restaurant Association

Analysis Prepared by: Thomas Clark / JUD. / (916) 319-2334